



Cert4Prep
Practice Test Software

VMware

3V0-25.25

Advanced VMware Cloud Foundation 9.0 Networking

Version: 6.0

Questions & Answers DEMO PDF

(Preview content before you buy)

Check the full version using the link below

<https://cert4prep.com/exam/3v0-25.25>

Unlock Full Features

Stay Updated: 90 days of free exam updates

Zero Risk: 30-day money-back policy

Instant Access: Download right after purchase

Always Here: 24/7 customer support team

Question 1. (DRAGDROP)

An administrator has noticed that both the active and standby Global Managers have gone offline.

What is the correct sequence of events to restore the Global Managers?

Delete both the active and standby Global Managers. Ensure there are no Global Manager appliances up in any other clusters.

Deploy a new Global Manager with the same IP address/FQDN as the old active Global Manager.

Restore the active Global Manager from backup.

Deploy an additional new Global Manager on another site and onboard it to the restored Global Manager.

The right column contains four empty green rectangular boxes for dragging the instructions into the correct sequence.

Answer:

Delete both the active and standby Global Managers. Ensure there are no Global Manager appliances up in any other clusters.

Deploy a new Global Manager with the same IP address/FQDN as the old active Global Manager.

Restore the active Global Manager from backup.

Deploy an additional new Global Manager on another site and onboard it to the restored Global Manager.

Delete both the active and standby Global Managers. Ensure there are no Global Manager appliances up in any other clusters.

Deploy a new Global Manager with the same IP address/FQDN as the old active Global Manager.

Restore the active Global Manager from backup.

Deploy an additional new Global Manager on another site and onboard it to the restored Global Manager.

Question 2. (ORDERLIST)

An administrator was asked to explain the characteristic and requirements of Centralized Connectivity Mode which is planned to be configured in one of the workload domains in

VMware Cloud Foundation (VCF) environment.

Drag and drop four options from the Options list on the left and place them into the Centralized Connectivity Mode on the right in any order. (Choose four.)

Options

- Requires a dedicated VLAN and subnet to connect the Transit Gateway with the ToR switch.
- It can be configured after the creation of a workload domain.
- Requires the deployment of an NSX Edge cluster to host the Tier-0 gateway.
- It can be configured during the deployment of the workload domain.
- It supports stateful services configuration.
- It is suitable for environments where that require a streamlined network with limited NSX networking services.
- It is required to use All Apps Org functionality in VCF Automation.
- DHCP and external IP services are the only services supported in this mode.

Centralized Connectivity Mode



A: Requires a dedicated VLAN and subnet to connect the Transit Gateway with the ToR switch.

B: It can be configured during the deployment of the workload domain.

C: Requires the deployment of an NSX Edge cluster to host the Tier-0 gateway.

D: It can be configured during the deployment of the workload domain.

E: It is suitable for environments that require a streamlined network with limited NSX networking services.

F: It supports stateful services configuration.

G: DHCP and external IP services are the only services supported in this mode.

Answer: A, D, F, E

Question 3. (Multi Select)

A large multinational corporation is seeking proposals for the modernization of a Private Cloud environment. The proposed solution must meet the following requirements:

- Support multiple data centers located in different geographic regions.
- Provide a secure and scalable solution that ensures seamless connectivity between data centers and different departments.

Which three NSX features or capabilities must be included in the proposed solution? (Choose three.)

A: NSX Edge

B: AVI Load Balancer

C: vDefend

D: Virtual Private Cloud (VPC)

E: Centralized Network Connectivity

F: NSX L2 Bridging

Answer: A, C, D

Explanation:

Comprehensive and Detailed 250 to 350 words of Explanation From VMware Cloud Foundation (VCF) documents:

In a modern VMware Cloud Foundation (VCF) architecture, particularly when addressing the needs of a multinational corporation with geographically dispersed data centers, the solution must prioritize multi-tenancy, security, and consistent delivery. The integration of NSX within VCF provides these core pillars.

First, the NSX Edge is a foundational requirement for any multi-site or modern cloud environment. It serves as the bridge between the virtual overlay network and the physical world. In a multi-region deployment,

NSX Edges facilitate North-South traffic and are essential for supporting features like Global Server Load Balancing (GSLB) or site-to-site connectivity. Without the Edge, the software-defined data center (SDDC) cannot communicate with external networks or peer via BGP with physical routers.

Second, vDefend (formerly known as NSX Security) provides the advanced security framework required for a "secure and scalable" environment. This includes Distributed Firewalling (DFW), Distributed IDS/IPS, and Malware Prevention. For a corporation with different departments, vDefend allows for micro-segmentation, ensuring that a security breach in one department's segment cannot move laterally to another. This is critical for meeting compliance and isolation requirements across global regions.

Third, the Virtual Private Cloud (VPC) model is the cornerstone of the latest VCF 9.0 and 5.x architectures. It enables the "scalable solution" for different departments by providing a self-service consumption model. Each department can manage its own isolated network space, including subnets and security policies, without needing deep networking expertise or constant tickets for the central IT team. This abstraction simplifies management across multiple data centers and allows for consistent application of policies regardless of the physical location.

While AVI Load Balancer and Centralized Network Connectivity are valuable, they are often considered add-ons or outcomes rather than the core architectural features that define the multi-tenant, secure, and geographically distributed nature of a modern VCF private cloud modernization project.

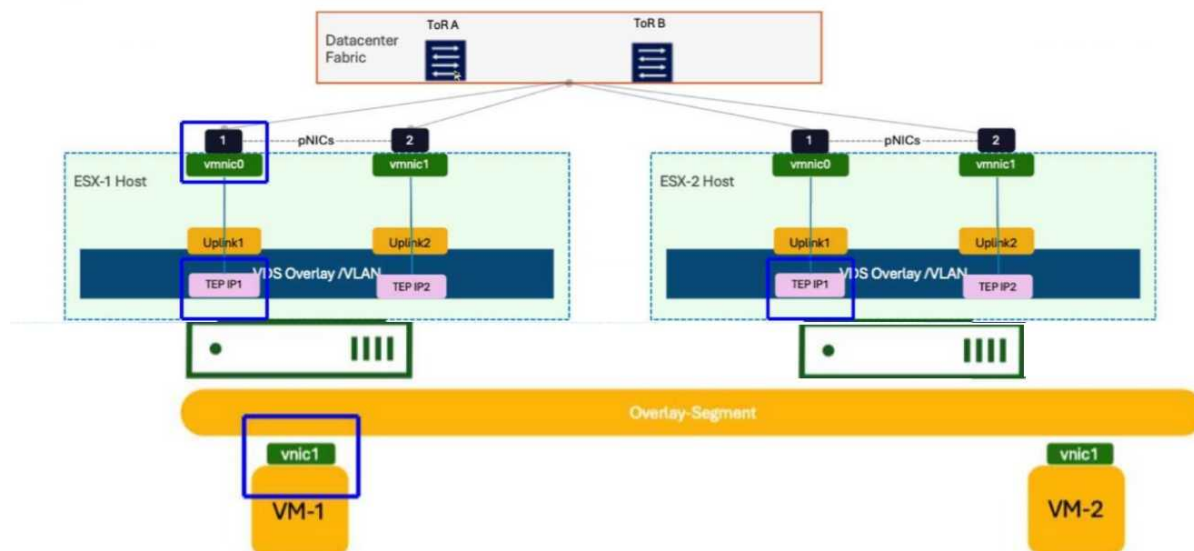
=====

Question 4. (HOTSPOT)

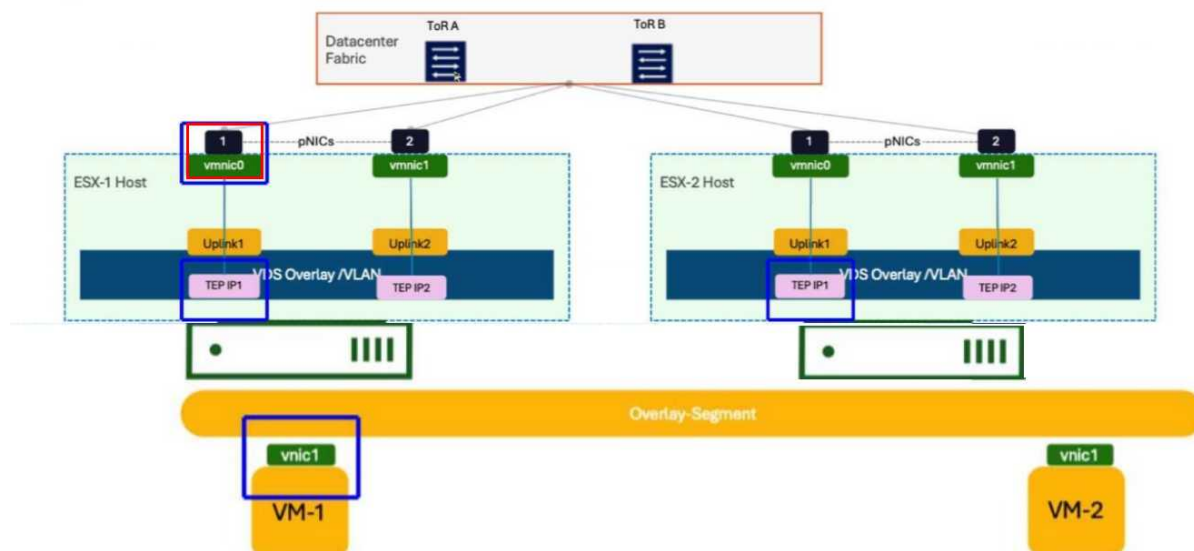
The administrator is working to ascertain the encapsulation of GENEVE by reviewing the capture on Wireshark.

The administrator instructed VM-1 to send a continuous ICMP request directed at VM-2.

Click to highlight where the administrator should observe the GENEVE encapsulated packet.



Answer:



Question 5. (Single Select)

An administrator has noticed an issue in a freshly deployed VMware Cloud Foundation (VCF) environment where the BGP neighborship between the Tier-0 gateway and a physical router remains in the Idle state. Pings between the uplink IPs are successful. What is the issue?

- A: Autonomous System number mismatch.
- B: Distributed Firewall blocking traffic.

- C: Geneve tunnel down.
- D: Overlay MTU too low.

Answer: A

Explanation:

Comprehensive and Detailed 250 to 350 words of Explanation From VMware Cloud Foundation (VCF) documents:

In the context of VMware Cloud Foundation (VCF), particularly versions 5.x and the architectural advancements in VCF 9.0, the establishment of North-South routing via the NSX Tier-0 Gateway is a critical post-deployment or bring-up task. The Tier-0 gateway uses Border Gateway Protocol (BGP) to peer with physical Top-of-Rack (ToR) switches to exchange reachability information for the overlay networks. When a BGP session is reported in the "Idle" state, it indicates that the BGP Finite State Machine (FSM) is at its first stage and is not yet attempting a TCP connection, or it has encountered an error that forced it back to this state. According to VMware VCF documentation and NSX troubleshooting guides, if the administrator can successfully ping between the Tier-0 uplink IP and the physical router interface, Layer 3 reachability is confirmed. This eliminates issues related to physical cabling, VLAN tagging on the trunk ports, or basic IP interface configuration.

The primary reason a BGP session remains Idle despite successful ICMP reachability is a configuration mismatch. Specifically, an Autonomous System (AS) number mismatch is the most frequent culprit. BGP requires that the "Remote AS" configured on the Tier-0 gateway matches the "Local AS" of the physical peer. If the SDDC Manager automated workflow or the manual configuration in NSX Manager contains a typo in these values, the protocol handshake will fail immediately.

While a Distributed Firewall (DFW) could technically block port 179, it is not common in a "freshly deployed" environment for the default rules to block the Edge Node's control plane traffic. Geneve tunnels and MTU issues (Option C and D) typically affect the data plane—causing packet loss for encapsulated guest VM traffic—but they do not prevent the BGP control plane (running over standard TCP) from moving beyond the Idle state. Therefore, verifying the AS numbers in the VCF Planning and Preparation Workbook against the physical switch configuration is the verified resolution path.

Need more info? Check the link below:

<https://cert4prep.com/exam/3v0-25.25>

Thanks for Being a Valued Cert4Prep User!

Guaranteed Success Pass Every Exam with Cert4Prep.

Save \$15 instantly with promo code

LEARN15

Sales: sales@cert4prep.com

Support: support@cert4prep.com

